The Software Alliance

BSA

Strengthening Trust, Safeguarding Digital Transformation

BSA'S CYBERSECURITY AGENDA

OCTOBER 2021

Modern society is built on software—it connects people to their friends and family, enables businesses to operate more efficiently and securely, and underpins the global economy. In the response to the COVID-19 pandemic, software was essential in enabling remote learning, working, and healthcare. Software is also shaping our future, driving 5G wireless networks, the Internet of Things (IoT), blockchains, and artificial intelligence.

As our digital transformation continues, it is imperative that enterprises and policymakers consider cybersecurity from the outset, as well as how these technologies can support broad and inclusive growth, as they develop and deliver the secure products and services that improve our lives.

Importantly, digital transformation is not solely about "ones and zeroes" but building stronger communities. The enterprise software industry supports good-paying jobs of the future in industries far beyond the technology sector; for example, as the BSA Foundation found, in the US alone, "In 2020, software supported more than 15.8 million jobs in total—an increase of 5.9 percent since 2018."

BSA is the leading advocate for the global enterprise software industry, and BSA members create the software products and services that power enterprises and improve lives around the world. They offer software that generates efficiencies and promotes trust and security, including cloud computing, customer relationship management, human resources management, and identity and access management products and services. Businesses trust BSA members to securely handle their most sensitive information, and BSA members' business models do not depend on monetizing consumers' personal data.

PRIORITIES TO IMPROVE CYBERSECURITY

Robust Software Security

Cybersecurity for Emerging Technologies

Modernization of Government IT and Cybersecurity

Interoperable Cybersecurity Laws and Policies Across Borders

An Effective Cybersecurity Workforce

BSA identifies the following priorities and offers policy recommendations for governments around the world to consider when seeking to improve cybersecurity.

Robust Software Security

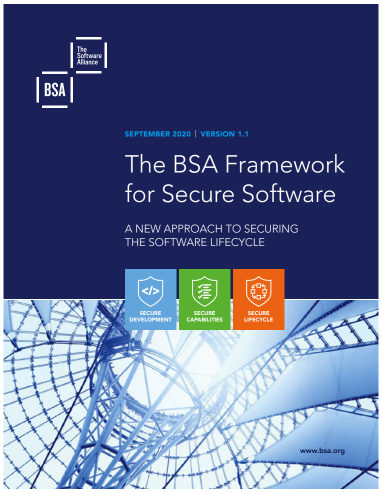
Managing software security risks must be a continuous improvement process because modern software, frequently delivered as a service, is commonly patched and improved daily and because adversaries continuously improve their tactics, techniques, and procedures. Industry has developed valuable tools and best practices that any organization can use to accelerate its improvement, including the BSA Framework for Software Security, a flexible, outcome-focused approach mapped to best practices and international standards.

BSA SUPPORTS

» Evaluating software security, including application security, using a lens of continuous improvement that considers (a) the development process, (b) built-in capabilities, and (c) lifecycle management. In contrast, laws and policies built on point-in-time assessments, such as labels or software bills of materials, can be a part of a broader program to improve cybersecurity but have limited value and may provide a false sense of security, particularly for cloud services. For further information on secure software approaches and methodologies, see the BSA Framework for Software Security.

» Using public-private partnerships to design laws and policies that improve software cybersecurity risk management rather than only creating a compliance mindset and accompanying checklists.

BSA RESOURCES



The Software Alliance
BSA

SEPTEMBER 2020 | VERSION 1.1

The BSA Framework for Secure Software

A NEW APPROACH TO SECURING THE SOFTWARE LIFECYCLE

SECURE DEVELOPMENT
SECURE CAPABILITIES
SECURE LIFECYCLE

www.bsa.org

The Software Alliance
BSA

Building a More Effective Strategy for ICT Supply Chain Security

Executive Summary

The Biden Administration and the 117th Congress should take a new, more effective approach to Information and Communications Technology (ICT) supply chain security. That process should begin by pausing and assessing the inventory of US supply chain security rules to move forward more effectively with a holistic and sustainable set of policies to improve security.

There are significant supply chain security threats from both government and non-governmental actors. In response to recent foreign government intrusions into US networks, the Biden Administration proposed significant investment in the Technology Modernization Fund to begin the hard work of moving toward a more secure digital ecosystem.

Global ICT supply chains continue to be important for the digital economy, but we need a modernized approach to supply chain security. In recent years, unfortunately, the government's actions have lacked a strategic focus and the articulated rationales for actions have been muddled—often conflating economic and national security objectives. Current policies are primarily based on intervention or country-based limitations. These policies are largely reactive, and they are often overly broad to the point where they become counterproductive to both security and economic growth.

In this white paper, BSA calls for a shift in emphasis to an assurance-based approach, coordinated across government agencies with a strategic focus. Assurance policies create incentives for companies to adopt best practices and improve the technology used to protect the supply chain. They are focused on risk-management that is more nuanced and tailored to the current environment, and more agile to adapt to future threats, than interventionist approaches.

The US government should reassert itself as a leader on security issues, working in both formal and informal alliances to improve collaboration with like-minded countries and create the global approach needed for success. Public-private partnerships, which, among other things, can create high-level standards and norms, is an important part of this approach.

BSA calls for a shift in emphasis to an assurance-based approach, coordinated across government agencies with a strategic focus.

www.bsa.org | 1

The Software Alliance
BSA

BSA Policy Principles for Building a Secure and Trustworthy Internet of Things

The evolving nature of the internet is creating new opportunities to connect devices, applications, and services on a scale that will transform daily interactions with our physical environment, work, and society. The Internet of Things (IoT) carries enormous potential to change the world for the better. Projections for the impact of the IoT on the internet and the global economy are significant, forecasting explosive growth in the number of IoT devices and their use in various applications. Globally, machine-to-machine (M2M) connections, which include IoT, will more than double in the coming years, from 6.1 billion in 2018 to 14.7 billion by 2023.[1]

Global M2M Connection Growth (in Billions of Connections)

19% Compound Annual Growth Rate

2018	2019	2020	2021	2022	2023
6.1	7.4	8.9	10.6	12.5	14.7

Source: *Cisco Annual Internet Report (2018–2023).*

Globally, machine-to-machine (M2M) connections, which include IoT, will more than double in the coming years, from 6.1 billion in 2018 to 14.7 billion by 2023.

Billions of IoT devices, applications, and services are already in use, with more coming online each day, and every new device can expand opportunities for malicious actors to disrupt the digital ecosystem. Some estimates conclude that cyberattacks on IoT devices in the first half of 2019 increased by 300 percent compared to the second half of 2018.[2] As the IoT continues to grow, IoT security is therefore of the utmost importance.

[1] Cisco, *Cisco Annual Internet Report (2018–2023)*, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

[2] F-Secure, *Attack Landscape H1 2019*, https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf; see also Zak Doffman, "Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims," *Forbes* (September 14, 2019), https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#220ecd435892.

www.bsa.org | 1

Cybersecurity for Emerging Technologies

Developing and harnessing emerging technologies requires strong cybersecurity. Just as a house built on a weak foundation will eventually crumble necessitating costly repairs, emerging technologies built without actively managing cybersecurity risks will face a similar fate. These innovations could bring transformational benefits, but require sufficient upfront security investments to help ensure emerging technologies do not serve as entry points for cyberattacks.

BSA SUPPORTS

» Developing laws and policies that are risk-based and appropriately tailored to allow for innovation, as well as deliver concrete cybersecurity improvement, and limit unintended consequences.

» Advocating 5G networks designed, built, operated, and updated with cybersecurity as a primary concern, while ensuring laws and policies promote competition.

» Leveraging automation to improve cybersecurity by, for example, enabling cybersecurity experts to more effectively focus on high-value tasks.

» Managing cybersecurity risks to the supply chain and IoT through a holistic approach, built on best practices and international standards where applicable. For more information on supply chain security and IoT, see BSA's white paper Building a More Effective Strategy for ICT Supply Chain Security and BSA Policy Principles for Building a Secure and Trustworthy Internet of Things.

Modernization of Government IT and Cybersecurity

Supporting governments by providing secure, trusted, and effective solutions is what BSA members do. By improving their own IT and cybersecurity, governments can improve the entire cybersecurity ecosystem.

BSA SUPPORTS

» Investing in the long-term security of government IT and cybersecurity, which will, over the medium and long term, save resources and better protect citizens.

» Improving government cybersecurity by migrating to cloud services, and implementing strong identity and access management practices, such as using zero trust architecture and multifactor authentication as many organizations have prioritized, including the US Government through the Executive Order on Improving the Nation's Cybersecurity.

» Advocating laws and policies that provide flexibility to ensure short-term government improvements do not ultimately result in governments receiving products and services that do not keep pace with the state of the art.

» Assisting state or provincial and local governments in modernizing their IT and improving their cybersecurity, including through financial support from national governments, as state or provincial and local governments often lag behind both private-sector organizations and national governments.

» Streamlining procurement processes and requirements to eliminate those that create undue burdens or do not concretely advance cybersecurity.

Interoperable Cybersecurity Laws and Policies Across Borders

Investing to ensure compliance with laws and policies constrains an organization's ability to invest in improving cybersecurity. Many countries have, or have proposed, laws and policies that require overlapping or duplicative requirements. For example, laws and policies requiring labels for software or IoT devices necessitate resources to implement that could be better invested in cybersecurity. Further, some countries' requirements are either not aimed at or do not have the effect of improving cybersecurity, but rather function as non-tariff trade barriers, such as many cloud security certifications; in such situations, the requirements harm the security of customers, countries, and the entire digital ecosystem.

BSA SUPPORTS

» Aligning laws and policies, for example those that require or propose to require incident reporting, so that, rather than spending resources on compliance, organizations can invest to improve cybersecurity.

» Ensuring cybersecurity laws and policies improve cybersecurity and are not, in reality, non-tariff trade barriers.

An Effective Cybersecurity Workforce

Building a secure future is not possible without developing an effective cybersecurity workforce. Increasing the pipeline of workers with the skills to meet government's and industry's demands is critical to continued economic growth. Importantly, many cybersecurity jobs do not require post-graduate, four- or even two-year degrees but can be completed by people who have earned applicable certifications. Fortunately, many people of all ages and from all walks of life have the aptitude and interest to learn these valuable cybersecurity skills.

BSA SUPPORTS

» Broadening opportunities, improving training programs, and expediting the development of the diverse workforce needed to secure our shared future.

» Promoting alternative paths to cybersecurity careers, for instance through apprenticeship programs, community colleges, "boot camps," and public service, and establishing mid-career retraining programs to provide workers with high-demand cybersecurity skills.